AIR WAR COLLEGE

AIR UNIVERSITY

NOT ALL PARTS ARE CREATED EQUAL.

THE IMPACT OF COUNTERFEIT PARTS IN THE AIR FORCE SUPPLY CHAIN

by

Bryan T. Horvath, LtCol, USMC

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: (Col Shelley B. Kavlick)

6 April 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Bryan T. Horvath is a Marine Corps Aircraft Maintenance Officer assigned to the Air War College, Air University, Maxwell AFB, AL. LtCol Horvath has served in the Marine Corps for more than twenty-five years both enlisted and as a commissioned officer. LtCol Horvath was commissioned a Second Lieutenant in February 1997 following graduation from California State University Fullerton. He most recently served as the Commanding Officer of Marine Aviation Logistics Squadron-14. He has served in a variety of staff positions including a recruiting tour and a joint assignment with United States Pacific Command. LtCol Horvath's operational experiences include deployments to Afghanistan, Iraq and a Western Pacific deployment aboard the aircraft carrier USS John C. Stennis.

Abstract

The existence and the volume of counterfeit parts residing within the Department of Defense's and in particular the United States Air Force's supply chain is real. Additionally, the disproportionate numbers of legacy aircraft in operation today and in the near future continue to complicate the issues. These legacy aircraft have long life cycles, diminished manufacturing sources, and frequent material shortages. Combine all these factors and you have a target rich environment for counterfeiting that will continue to escalate as long as it is profitable.[1] Counterfeit parts have been polluting the DOD supply chain since the 1990s. There are various reports, news and magazine articles on the subject, but it was not until Congress made significant legislative changes in the National Defense Authorization Act (NDAA) of 2012 has action been taken to mitigate and reduce counterfeit parts in the DOD supply chain. Since 2012, the U.S. Government implemented a whole of government approach to tackle this issue. This issue affects both DOD, defense contractors by increasing costs, reliability, and theft of intellectual property, and could ultimately results in the death of a military member. This paper will examine the background on counterfeiting and the potential impacts such as increased cost, poor reliability, or catastrophic consequences. Additionally, current laws, orders, and instructions from the DOD as well as the United States Air Force will be reviewed with respect to relevancy of the counterfeit part mitigation solutions. Finally, the report concludes, the overall impact that the Air Force controls is negligible because of costs, limited resources, and numerous factors most of which are outside the control of the Air Force. The U.S. Government should establish policies limiting electronic waste disposal and implementing acquisition policies that focus on best value vice awarding acquisition contracts to the lowest cost.

Introduction

The Air Force supply chain continues to be a target for counterfeit parts either for criminal purposes or for malicious code intent. Counterfeit parts have been polluting the Department of Defense (DOD) supply chain since the 1990s. There are various reports, news and magazine articles on the subject, but it was not until Congress made significant legislative changes in the National Defense Authorization Act (NDAA) of 2012 has action been taken to mitigate and reduce counterfeit parts in the DOD supply chain. Since 2012, the U.S. Government implemented a whole of government approach to tackle this issue. According to a Government Accountability Office (GAO) report released in February 2016, "DOD needs to improve on reporting and oversight to reduce Supply Chain Risk".[2] In other words, the issue has not been resolved. This issue affects both DOD, defense contractors by increasing costs, reliability, and theft of intellectual property, and could ultimately results in the death of a military member. This paper will examine the background on counterfeiting and the potential impacts such as increased cost, poor reliability, or catastrophic consequences. Additionally, current laws, orders, and instructions from the DOD as well as the United States Air Force will be reviewed with respect to relevancy of the counterfeit part mitigation solutions. Finally, the report will offer policy recommendations for additional steps the U.S. Government should implement to reduce further the number of counterfeit parts in the supply chain.

Thesis

The Air Force has implemented policies or procedures to mitigate the risk of counterfeit parts in the supply chain. However, the counterfeit problem is larger than the Air Force and requires a combined government and industry solution in order to reduce the amount of counterfeit parts in the supply chain.

Background

Counterfeit parts are not a new phenomenon of the twenty-first century. The trade of creating and manufacturing counterfeit parts has existed since men began trading goods more than 2,000 years ago. Early on, religious leaders from ancient Egyptian and Babylonian era placed certain markings on buildings as an effort to certify their legitimacy and thus increase offerings. Ancient Chinese and Greeks used special marks to identify their pottery and in Japan, lumber was marked to identify ownership.[3] All of these early examples created opportunities for counterfeiting in order to increase profits or prestige. In the United States, cotton was one of the earliest products counterfeited. William Eleroy Curtis, wrote, "the superiority of American [cotton] goods is so great that the Manchester [England] mills send few goods to South America that do not bear a forged American trademarks."[4]

Fast forward to late in the twentieth century, a 'wicked problem' similar to that of an iceberg is in a direct path towards the integrity and reliability of the military supply chain. Unlike other industries, counterfeiting in the aerospace industry has the potential for life or death consequences. Since the mid-1980s the U.S. defense industry has undergone a transformation into a global defense industrial base. For example, "The number of major U.S. –based defense and aerospace companies shrunk from 21 in 1993 to six today."[5] Additionally, the defense industry made up 26 percent of the demand for semiconductors in the late 80s; in 2008, that number plummeted to less than 0.1 percent. Furthermore, production life cycles for electronic components have shrunk to less than 2 years.[6] In conclusion, then the combination of decreased demand on electronics manufactures of military grade components and short production life make it virtually impossible for the Department of Defense to build and maintain systems for decades.

In addition to the previous cause and effect, factors influencing the decline in U.S. based defense industry, the push for increased use of commercial off-the-shelf products began with the Clinton administration and continued through Bush's administration.[7] Furthermore, the DOD began ordering parts from small U.S. parts distributors that sprang up virtually overnight after Congress did away with requiring primary government contractors to certify all components came from original manufactures or authorized distributors. Because of federal affirmative-action goals, the military purchased parts from business labeled as "disadvantaged" many of which operated out of the private residence with little or no oversight once they received their contractor code. These brokers would comb websites in search of parts on the wholesale market oftentimes fulfilling their orders from suppliers located in China.[8] Therefore, virtually all U.S. weapons systems built today contain foreign parts, maintained with foreign parts, and setting the perfect conditions for counterfeiters to thrive.

Another factor influencing the rise in counterfeit parts stems from the increase in electronic waste commonly referred to as E-waste, and the improper disposal of that waste. Electronic waste is, "any refuse consisting of discarded electronic devices and components, new or old, functioning or non-functioning."[9] Several studies conducted over the last ten years documented E-waste as a primary source for electronic counterfeit parts. The reason for this is twofold. First, counterfeiters have the potential to make a large profit. Second, the availability of E-waste continues to grow because environmentally conscience modern countries recycle their electronic components to include the United States military.[10] These studies documented shiploads of E-waste going to countries in West Africa as well as China. The counterfeit parts industries takes scrap electronic circuit cards and place them over open flames, loosening the individual components as well as releasing toxic chemicals into the environment.[11] Once the

individual components are removed from the circuit boards they are normally washed in the local river or left outside in the rain and once dried shipped to larger facilities that prepare the components for counterfeiting. At the larger facility, parts are sanded and or put through an acid wash to remove identifying marks, then resurfaced, this process is known as "blacktopping". "Blacktopping" designed to hide old markings and allows for new markings. The Guangdong Province in China is the epicenter for counterfeiting activities in China.[12] This process has the potential for catastrophic consequences because electronic components are sensitive to moisture, static electricity, improper handling and the acid damages the components resulting in the parts failing sooner. These counterfeit parts are often identified as new by the counterfeiters and sold back to U.S. companies. Another area of concern is China's capability to produce new counterfeit components that could incorporate malicious code that would be able to conduct a cyber attack.[13] Although this is possible, it is unlikely because of the complexity of the electronic components would prevent the multi-functionality of the component as cause it to fail during testing. Government and the electronic industries need to work together in order to develop policies that limit or restrict the flow of E-waste out of the United States.

What constitutes a counterfeit part?

In discussion of counterfeit parts, one controversial issue has been the definition of a counterfeit part. On the one hand, some in industry define a counterfeit part as an unauthorized copy of an authentic product or a mislabeled product. On the other hand, some in Congress leading up to the NDAA 2012 wanted to include any parts with high failure rates.[14] In 2010, the Department of Commerce defined counterfeit parts as follows:"

- Unauthorized copy

- Does not conform to Original Component Manufacturer (OCM) design, model, or performance standards
- Not produced by the OCM or by its authorized contractors
- Off-specification, defective, or used OCM product sold as "new" or working
- Incorrect of false markings [or] documentation."
- May include: recycled aged or nonfunctional parts, remarked new or recycled components, selling overproduced Integrated Circuits (IC) outside of the authorized supply chain, or selling out-of-spec components, cloned parts by pirated Intellectual Property (IP) or by reverse engineering, ICs reproduced with tampered designs (which can implement hardware-based security breaches), or components sold with forged documentation."[15]

The latter definition became widely used by most agencies within the Department of Defense however, some organizations created their own. For example, during an investigation in 2010 the Government Accountability Office noted, "one DLA supply center defined a part as counterfeit only when it misrepresented the part's trademark. In contrast, a different DLA supply center defined counterfeit parts more broadly to include misrepresentations of a part's quality and performance."[16] Still others were unsure if this definition only applied to electronic components or carried over to other parts like nuts, bolts, and tires.

At the conclusion of an extensive yearlong investigation by the House Armed Service Committee (HASC) in 2011 on counterfeit parts, Section 818 of the 2012 NDAA directed DOD to define suspect and confirmed counterfeit electronic parts, as well as implement a DOD issued its Counterfeit Prevention Policy in April 2013.[17] According to DOD Counterfeit Prevention Policy, counterfeit materiel is, "an item that is an unauthorized copy or substitute that has been

identified, marked, or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source. And suspect counterfeit material, items, or products in which there is an indication by visual inspection, testing, or other information that it may meet the definition of counterfeit materiel."[18]

Even after DOD published the official definition of counterfeit materiel, the Air Force defined counterfeit materiel as, "materiel whose identity or characteristics were deliberately misrepresented, falsified, or illegally altered."[19] I believe this oversight must have been an error since the DOD definition preceded the Air Force's by approximately six months. The current Air Force Instruction on Materiel Management updated in December 2016 matches the DOD definition.[20]

Ultimately, what is at stake here is the importance for government and industry to agree upon a universal definition on what constitutes a counterfeit part and handle accordingly.

Background investigation finds rapid growth in counterfeit electronics from 2005 to 2016

Over the last 40 years, military equipment has become increasingly dependent on electronic parts to enable their advanced capabilities. For example, the F-35 Joint Strike Fighter, the U.S.'s next generation multi-role fighter, currently in production, contains more than 3,500 integrated circuits, therefore opportunities for counterfeit components exists because of more sub-contractors increasing more vulnerabilities in the supply chain.[21] At the same time that our military systems have become more reliant on electronic parts, global forces responsible for the dramatic increase in consumer counterfeits have also affected the aviation and defence industries. A 2016 report from the U.S. Chamber of Commerce cites a study conducted by Organization for Economic Co-operation and Development (OECD) estimating that, "global trade-related counterfeiting accounts for 2.5 percent of world trade, or 461 billion U.S.

Dollars."[22] This is an increase of 55 percent in less than 10 years. Counterfeit parts of all types have been found across the DOD. This is significant because the safety of American service personnel lives is at stake when the integrity of aircraft parts is being compromised in the supply chain. Two reports that drove action by Congress and the executive branch were the 2010 U.S. Department of Commerce report and Senate Armed Service Committee (SASC) report released in 2012. Both reports had a direct impact on the 2012 NDAA.

2010 U.S. Department of Commerce report

At the request of the U.S. Department of the Navy, Naval Air Systems Command (NAVAIR) the U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation conducted a defense industrial base assessment of counterfeit electronics. The results of the findings indicated the number of counterfeit parts in electronics military components more than doubled between 2005 and 2008, growing from 3,868 incidents to 9,356 incidents.[23] The report surveyed 387 organizations across the supply chain, including original component manufacture (OCM), distributors and brokers, circuit-board assemblers, prime and subcontractors, and DOD supply agencies. Survey respondents attributed the increase to a number of factors to the increase in the number of counterfeit parts, such as better detection methods and improved tracking of incidents. Additionally, the report recommended seven actions the U.S. Government could take in order to slow down the inflow of counterfeit parts into the military supply system.[24]

2012 U.S. Senate Armed Service Committee (SASC) report

In early 2012, the SASC released a detailed report capturing the impact of counterfeit parts in the military supply system, identifying huge gaps in current laws and provided eight conclusions to mitigate future risks. The report consisted of congressional hearings by the SASC

that included testimony by industry experts and various companies, the Commerce Department finding, an internal GAO report, and internal work by the committee.[25]

The committee uncovered 1,800 cases of suspect counterfeit parts representing over 1 million parts. The 1800 cases covered the period of 2009 through the 1st quarter of 2011 consisted of: 200 from DLA, 150 from various contractors, and 1,500 from several testing houses.[26] According to SASC ranking member Sen. John McCain, R-Ariz., "Our committee's report makes it abundantly clear that vulnerabilities throughout the defense supply chain allow counterfeit electronic parts to infiltrate critical U.S. military systems, risking our security and the lives of the men and women who protect it."[27] This matters because at the conclusion of the committee offered an amendment to the FY 2012 NDAA to address weaknesses in the defense supply chain and to promote the adoption of aggressive counterfeit avoidance practices by DOD and the defense industry. President Barrack Obama signed the final bill on December 31, 2011.[28]

Examples of counterfeit parts in the U.S. Air Force supply system

Fortunately, to date, there have been no attributed fatalities due to counterfeiting; although the list of affected weapon systems is extensive and includes components found in: F-15, F-16, F-22, B-52, C-130, C-5, and Joint Stars. Examples of components items range from: GPS receivers, microprocessors, electronic components, microcircuit components, fasteners, and various metals to name a few.[29] Prior to the two highly publicized investigations, various reports of counterfeit parts would appear in the news. One case reported occurred in January 2008 where a counterfeit chip was discovered in the flight computer of an F-15. Further investigation located four additional falsely marked chips located in a supply warehouse.[30] Another example occurred in November 2010, when L-3 Display Systems notified Lockheed Martin, the Air Force's prime contractor on the C-130J, that they identified more than 400 digital displays

contained counterfeit memory chips. Lockheed Martin never formally notified the Air Force but monitored the situation for six months that resulted in inconclusive data. To complicate matters further, it is one thing to identify a suspected counterfeit part but it is another herculean task to notify and take timely and appropriate actions. The C-27J transport aircraft failed Bus Adaptor Unit (BAU) is one such example. The BAU allows different systems to talk to one another, like the plane's anti-skid controller, de-icing system, and mission computer. In this case, it took more than two years from discovery to officially notifying the U.S. Air Force in August 2011.[31] This last example clearly identified how the lack of communication and timely action from manufactures put people's lives at risk.

Although the majority of the cases discovered in the SASC report came from testing houses, it is unclear the actual number of failures due to counterfeiting and what percentage failed up screen testing. Moreover, it is difficult to pin point valid cause and effect factors. For example, is there an actual growth in counterfeit parts flooding the supply system or is the system's detection rates increasing? These issues barely scratch the surface on the 'wicked problem' facing the DOD supply system.

Outcome of prosecuted counterfeit cases

Prior to the approval of the Combating Military Counterfeiting Act of 2011 bill, criminals selling counterfeit parts used in military components received the same punishment as someone selling or producing counterfeit shoes or other counterfeit consumer products. This bill, introduced by Senator Charles E. Schumer (D-NY) dramatically increased the maximum penalty for these types of offenses from 10 to 20 years acknowledging that counterfeit military components poses a more serious health and national security risk than most counterfeit consumer products.[32] In November 2005, an Orange County man sentenced to 16 years and

fined $5.4 million for selling counterfeit flight critical aircraft parts and offering to sell fighter plane parts to China. Khan plead guilty to 12 felony counts for falsely certifying aircraft parts for helicopters, F-16, and C-130 aircrafts.[33] A more recent case occurred in 2014 in which a Massachusetts man plead guilty to importing thousands of counterfeit integrated circuits from China and reselling them to the U.S. Navy for use in nuclear submarines. Testing by the Navy revealed the parts had been resurfaced and modified to hide the fact they were old used parts. Under the new law that went into effect in 2011, the man was sentence to 37 months in prison.[34] Perhaps Senator Schumer captures it best when he states, "criminals who have the audacity to put our troops at risk should not be treated the same as other con-artists; these heinous acts demand enhanced penalties."[35] Ultimately, what is at stake here is the safety of thousands of military members putting their lives on the line and should be protected at all cost, including better integrity in the supply chain to produce reliable parts.

The U.S. Government's role in reducing counterfeit parts

The U.S. Government and its numerous agencies along with industry all play a vital role in reducing counterfeit parts in the military supply chain. The tipping point occurred with the passage of the NDAA 2012. Along with the 2012 NDAA, various Department of Defense instructions, Air Force instructions and policy letters as well as the creation of the National Intellectual Property Rights Coordination Center (IPR Center) all designed to reduce the flow of counterfeit parts entering the military supply chain. After several in depth reports, hearings and conferences, the likelihood of preventing counterfeit parts 100 percent of the time is a bridge too far because it is expensive to test every single bit piece part, time consuming and even if the part passes the test it could be refurbished.

The NDAA 2012, specifically section 818 lays out the foundation to reduce the threat of counterfeit parts. As a forcing function, this law shifted the responsibility of the cost to replace counterfeit parts and cost directly tied to these actions down the entire supply chain. In other words, the contractors and their subcontractors will be held financially responsible for corrective actions . The primary change required contractors to only purchase from Original Equipment Manufacturers (OEM) and their authorized distributors. All parts must have a certificate of conformance (CoC) as well as a chain of custody certificate that is traceable back to the original manufacture if the part is from an authorized distributor.[36] Unfortunately, a large majority of replacement parts are no longer in production given the reality of the short production life span coupled with the military equipment service period. These cases require additional steps known as Counterfeit Electronic Part Avoidance (CEPA). The CEPA process requires component engineers evaluate potential component sources and imposes specialized testing to validate the components. This process must occur prior to actual purchase of the parts. The CEPA process may require that the proposed parts supplier's facilities be certified and monitored.[37] Finally, the law also required contractors and subcontractors to report counterfeit parts using the Government Industry Data Exchange Program (GIDEP) or some other designated counterfeit reporting system.

Section 818 also directed DOD to establish a department-wide definition of "counterfeit electronic part" as well as implement a risk-based approach to minimize the impact of counterfeit parts or suspect counterfeit electronic parts on the Department. Additionally, the law called for updated guidance on remedial actions for a supplier that routinely fails to detect and avoid counterfeit electronic parts.[38] In April 2013, the Department of Defense published DOD

Instruction on Counterfeit Prevention Policy, which established the roles and responsibilities for implementing the anti-counterfeiting strategy as well as GIDEP reporting for counterfeit parts.[39]

The Role of industry in reducing counterfeit parts

Industry plays a critical role in reducing counterfeit parts, since counterfeit parts are practically everywhere. Given the increasing amounts of counterfeit parts showing up in the complex supply chain over the past two decades, extra attention is required to ensure that the performance and authenticity of parts is not compromised. Many experts believe the most effective approach to avoid introducing counterfeit parts into the supply chain is not to purchase them in the first place. Since this is simply not possible, manufactures should avoid purchasing parts from independent distributors and brokers because this is where the greatest likelihood of receiving counterfeit parts exists. These same experts recommend parts should come directly from the original manufacture, or from a distributor, reseller, or aftermarket supplier authorized by the original manufacturer.[40] Several organizations consisting of industry and governmental agencies formed to develop standards and best manufacturing practices to reduce counterfeit parts entering the supply chain.

A good example of Industry and DOD collaboration is the Society of Automotive Engineers (SAE) International G-19 Counterfeit Electronic Parts Committee. SAE is a U.S. based globally active professional association and standards organization for engineering professionals. The SAE G-19 committee developed Aerospace Standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition released April 2009. The committee included representatives from DOD, NASA, the US Department of Homeland Security, prime contractors, component manufactures, contract assembly manufacturers, franchised distributors, independent distributors, and industry association representatives.[41]

AS5553 contains seven requirements to decrease the introduction of counterfeit parts into their supply chain. First, maximize the availability of authentic parts throughout product lifecycle; anticipate and manage obsolescence (significant challenge with military components). Next, only buy from Original Component Manufacturers (OCMs) or authorized distributors. Specify contract and purchase order quality requirements. Detect counterfeit parts through incoming inspection. Control suspected or confirmed counterfeit parts to prevent re-entry into supply chain. Finally, report counterfeit parts to customers, and other authorities, including use of Government-Industry Data Exchange Program (GIDEP). [42] This standard requires those who adopt it to develop and use a counterfeit electronic parts control plan. The control plan emphasizes the importance of procurement practices and product traceability, external auditing, and penalties associated with fraud.

In addition to the G-19 committee, SAE organized the G-21 counterfeit materiel committee that developed Aerospace Standard AS6174. AS6174 provides standardized requirements, practices, and methods to improve the likelihood of only acquiring authentic and conforming materiel of any type in any industry sector. SAE also developed AS6171 and AS6496. AS6171 created standardized practices to detect suspect counterfeit electronic parts and to ensure consistency of test techniques and requirements across the supply chain. AS6496 identifies uniform practices to procure, authenticate, track, and minimize risk of counterfeit parts in authorized supply chain.[43]

Detection Methods

Detecting counterfeit parts prior to purchasing and installing on components is the first priority with manufacturers. Currently no single test exists that will detect one hundred percent of counterfeit parts. Manufactures and suppliers rely on multiple testing methods in order to

increase detecting rates. The Independent Electronics Association (IDEA) is another international organization that seeks to provide responsible procurement solutions to the supply chain. IDEA developed "IDEA-STD-1010: Acceptability of Electronic Components Distributed in the Open Market".[44] IDEA-STD-1010 establishes standard operating procedures for visual inspection and evaluation criteria in order to aid in the detection of substandard and counterfeit components prior to purchasing in the open market.

The most common method of detecting counterfeits parts in the early part of the twenty-first century was through high failure rates. From there visual detection methods were introduced and the counterfeiters adapted with better "blacktopping (process of resurfacing a chip to cover over original markings) and improved marking methods".[45] The inability to visually identify and distinguish counterfeit parts from original parts led to industry developing costly and thorough destructive and non-destructive inspection methods. Some of the detection methods include the following: Scanning Electron Mircroscopy (SEM), Radiological, X-Ray Fluorescence (XRF), electrical tests, Acoustic Microscopy, Fourier Transform Infrared Spectroscopy (FTIR), RAMAN Spectroscopy, Thermo-gravimetric Analysis (TGA). Some of these tests take minutes and hours to perform while others take weeks. Additionally, the cost of detection equipment is another factor driving up the cost of electronic components. For example, a real time X-Ray machine costs around $350,000.[46] While detection methods improve, the same holds true to the counterfeiting methods.

Reporting requirements

The NDAA 2012, specifically section 818 requires contractors and subcontractors to report counterfeit parts using the GIDEP or some other designated counterfeit reporting system.[47] Prior to this reporting requirement becoming law, there were only 271 total reports submitted to

GIDEP out of the 1,800 cases of suspect counterfeit parts in the DOD supply chain during 2009 and 2010.[48] Multiple defense contractors and distributors told the SASC that they were hesitant to submit reports of suspected counterfeit parts to GIDEP in part due to fear of third party lawsuits. GIDEP requires the reporting company to name the supplier of a suspect part.[49] In April 2013, the Department of Defense published DOD Instruction on Counterfeit Prevention Policy, which established the roles and responsibilities for implementing the anti-counterfeiting strategy as well as GIDEP reporting for counterfeit parts.[50]In addition to GIDEP manufactures and DOD supply agencies use two other systems to report nonconforming parts. The Product Data Reporting and Evaluation Program (PDREP) is managed by the Navy and used by the Army, DLA, and DCMA. The other reporting system is the Joint Deficiency Reporting System (JDRS) primarily used by the Air Force and Naval Air Systems Command. Both systems allow the users to categorize the nonconforming parts as suspect counterfeit.[51]

In February 2016, the GAO released a report to Congress on counterfeit parts and how DOD needs to improve reporting and oversight in order to reduce supply chain risk. For fiscal years 2011 through 2015, 526 reports of suspect counterfeit parts submitted, with contractors submitting over 90 percent of the GIDEP reports. Additionally, a majority of the those reports occurred in 2011 and 2012 in part due to congressional attention to counterfeit parts prompting contractors to examine their inventory and identify previously undetected counterfeit parts. Others argue the increase in reporting compared to the following years is because of an amnesty period that allowed GIDEP reporting without naming a supplier. Still other government officials claim the lower number of reports after 2012 is the result of improved practices to prevent the purchase of counterfeit parts.[52] Furthermore, the Army, the Air Force, and the Missile Defense Agency (MDA) did not submit any suspect counterfeit GIDEP reports in this period. Air Force

officials explained, "that they have relied on their contractors to submit reports because they have the best knowledge of how and where the counterfeit part was procured."[53] In another example, the Air Force failed to report a debarred subcontractor in GIDEP for supplying counterfeit electronics parts. Once again, Air Force officials stated, "that its prime contractor submitted related suspect counterfeit GIDEP reports" however those reports failed to include the name of the debarred subcontractor.[54] This example highlights the disconnect in overall reporting and by failing to include critical information the entire system fails to provide the pertinent information to raise awareness of the problem. The report concluded with four recommendations for the Undersecretary of Defense for Acquisition, Technology and Logistics. First, the report recommended creating a mechanisms providing department-wide oversight of defense agencies' adhering to the GIDEP reporting requirements. Second, develop a standardized process for the amount and type of evidence required in order to report a part as suspect counterfeit in GIDEP. Third, provide guidance for when to limited GIDEP reports to only government users. In addition, the final recommendation in the report is to provide industry with a set of standards used to evaluate a contractor's counterfeit detection and avoidance system.[55]

Recommendations

The existence and the volume of counterfeit parts residing within the DOD's and in particular the United States Air Force's supply chain is real. Additionally, the disproportionate numbers of legacy aircraft in operation today and in the near future continue to complicate the issues. These legacy aircraft have long life cycles, diminished manufacturing sources, and often frequent material shortages. Combine all these factors and you have a target rich environment for counterfeiting that will continue to escalate as long as it is profitable.[56] Since the enactment

of the 2012 NDAA and subsequent modifications over the last five years, the United States government continues to attack the issue. Although legislation alone will not solve this issue instead, it will take a collaborative effort from various government agencies and industries partners both foreign and domestic to reduce the amount of counterfeits parts within the DOD's and U.S. Air Force's supply system.

Because counterfeit parts prevention is bigger than the Air Force or the United States government stakeholders for that matter, it is short sided to think the Air Force could solve this issue alone. As of December 2016, with the publishing of Air Force Instruction 23-101 on Air Force Materiel Management, the Air Force has in place policies and procedures to decrease the amount of counterfeit parts in the supply chain for legacy aircraft as well as newly procured aircraft. Detecting counterfeit parts will remain a challenge in part due to limited resources both in money and replacement assets on the supply shelves. Specifically, when a part checks bad on an aircraft, it is removed and inducted for repair; not put to the side as a suspected counterfeit part. Because of this fact, it is virtually impossible to accurately measure the impact counterfeit parts are having on the Air Force supply system. It is possible for counterfeit parts to put into higher assembly and check good during post maintenance action specified testing. The potential impact is reduced reliability or possible inflight failure. This is one area where the Air Force procurement professionals can weigh-in. Air Force Instruction 63-101/20-101 specifically tasks program managers to, "identify and maintain an updated list of critical components vulnerable to counterfeiting throughout the system life cycle."[57] In other words, they need to prioritize systems or subsystems and recognize that not all risks are the same. By identifying critical parts, they can accept some risk because the impact of failure would be low.

One area in which Senior Air Force leadership as well as other members of DOD could positively affect the reduction of counterfeit parts is through key leader engagement with our elected officials and encourage them to pass additional legislation. Since 2014, Representative Paul Cook (R-CA) introduced legislation to "control the export of electronic waste in order to ensure that such waste does not become the source of counterfeit goods that may reenter military and civilian electronics supply chains in the United States, and for other purposes."[58] The bill is currently pending recommendations from a congressional committee before going forward. If made into law, this bill would reduce the amounts of e-waste shipped to Africa and China thus reducing material for counterfeiters to use. Several expert in industry identified the lack of regulations and oversight of the scrapping, recycling, and disposal of military parts as an avoidable source of counterfeiting. Specific practices that industry should incorporate to confirm that scrapped, excess, and suspected counterfeit materials are not used to make more counterfeit parts include:[59]

- Requiring suspect counterfeits to be quarantined upon detection
- Auditing suppliers to ensure proper tracking of the amount of scrapped material destroyed
- Requiring suppliers to use contract clauses that prevent the resale of scrap parts to third parties
- Witnessing the destruction of seized or returned counterfeit parts

In civil aviation, the Federal Aviation Administration published a best practice instruction for proper disposal of scrap or salvageable aircraft parts and materials. The manual recommends mutilation of scrap parts or materials to prevent reintroduction back into the supply system.

Cutting holes, sawing, melting, and removing manufacturer identification are a few of their recommendations.[60]

Although outside the scope of this research paper, the DOD needs to develop solutions that account for limited budgets and find an acceptable balance between risk and costs. DOD program managers should collaborate with program contractors to determine an appropriate, individualized, risk-based approach to counterfeit mitigation that adheres to established standards. Again, the program manager needs to apply both qualitative and quantitative processes when determining risk. Another action they could take is to debar suppliers who repeatedly furnish parts or components containing counterfeit parts. This would limit the impact of bad actors like Hong Dark Electronics. During the Senate Armed Service Committee an Air Force official stated, "Hong Dark Electronic Trade of Shenzhen, China supplied approximately 84,000 suspect counterfeit electronic parts into the DOD supply chain."[61] My final recommendation or suggestions are for DOD to focus on best value vice awarding acquisition contracts to the lowest cost. The reliance on lowest price technically acceptable (LPTA) comes with several second and third order effects. For example, companies offering a lower price may have less reliable supply chains, quality control processes, and less experienced employees all of which could end up costing more money in the end. In part due to less reliability of the component and may lead to increase incidents of counterfeits.[62]

Conclusion

According to a 2016 report from OECD estimated that, "global trade-related counterfeiting accounts for 2.5 percent of world trade, or 461 billion U.S. Dollars."[63] Because of obscene profits as suggested in this report, elimination of counterfeiting will remain a herculean

challenge for law enforcement, industry, and government stakeholders. In order to reduce this threat, the United States government, specifically the DOD and its industry partners will have to work together to reduce the risk to acceptable levels, at an affordable cost. This paper examined the background on counterfeiting and the potential impacts such as increased cost, poor reliability, or catastrophic consequences. It also examined currently laws, orders, and instructions from the DOD as well as the United States Air Force. Finally, the report offered several recommendations however, the overall impact that the Air Force controls is negligible because of cost, limited resources, and numerous factors most of which are outside the control of the Air Force such as control of electronic waste and acquisition policies that focus on best value vice awarding acquisition contracts to the lowest cost.

Notes

[1] Ron C. Ball, "The DoD Counterfeit Threat & Compliance." Paper for Keesler Aerospace Solutions, Orlando, FL, 2013, 5.

[2] Government Accountability Office, *COUNTERFEIT PARTS DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk.* GAO-16-236, Washington, DC: United States Government Accountability Office, February 2016, 2.

[3] Peggy, Chaudhry and Allan Zimmerman. *Protecting Your Intellectual Property Rights Understanding the Role of Management, Governments, Consumers and Pirates* (Springer, New York: Springer Science & Business Media, 2013), 8.

[4] Ibid., 9.

[5] Jacques S., Gansler, William Lucyshyn, and John Rigilano. *Addressing Counterfeit Parts in the DoD Supply Chain.* (Center for Public Policy and Private Enterprise. College Park, MD: University of Maryland, 2014), 5.

[6] Senate Committee On Armed Services. Inquiry Into Counterfeit Electronic Parts In The Department Of Defense Supply Chain. 112th Cong., 2nd Sess., 2012. S. Doc. 112-167. 24.

[7] Dr Gareth Evans, "*Flying fraudulently – how a weak supply chain became the USAF's worst enemy*." Airforce-technology.com, 2012. http://www.airforce technology.com/features/ feature supply-chain-us-air-force-fraudulent-parts/. 3.

[8] Brian, Grow, Chi-Chu Tschang, Cliff, Edwards and Brian Burnsed, "Dangerous Fakes." Bloomberg Businessweek, 1 October 2008. http://www.businessweek.com/stories/2008-10-01/dangerous-fakes. 3.

[9] *A Special Report Counterfeit Parts: Increasing Awareness and Developing Countermeasures* (Arlington, VA: Aerospace Industries Association, 2011) 28.

[10] IBID., 28.

[11] Andrew, Dobbs. *We Threw Military Electronics In the Trash – China Sold Them Back to Us: How E-Waste Compromises America War tech.* War is Boring, Accessed 24 September 2016. https://medium.com/war-is-boring/we-threw-electronics-in-the-trash-china-sold-them-back-to-us-d52e06111fff. 2.

[12] Jim, Burger, Henry Livingston, and Tom Sharpe. "Electronic Waste Rules could Help Thwart Flow of Counterfeit Parts." National Defense 99, no. 735 (02, 2015): 14-15. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url =http://search.proquest.com.aufric.idm.oclc.org /docview/1653124073?accountid=4332. 1.

[13] Hans M. Sassenfeld, *Counterfeit Prevention Strategies in the Military Supply Chain: Increasing Reliability at a Higher Price* (Capstone, University of Texas, El Paso, 2013), 5.

[14] IBID., 13.

[15] Department of Commerce. Defense industrial base assessment: Counterfeit electronics (Washington D.C.: Bureau of Industry and Security, January 2010) 3.

[16] Government Accountability Office, *DEFENSE SUPPLIER BASE DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Needs to Improve Reporting and Oversight to Mitigate Risk of Counterfeit Parts*. GAO-10-389, Washington, DC: United States Government Accountability Office, March 2010. 8.

[17] Senate Committee On Armed Services. Inquiry Into Counterfeit Electronic Parts, 8.

[18] DOD Instruction (DODI) 4140.67. *DOD Counterfeit Prevention Policy*, 26 April 2013, 12.

[19] Air Force Pamphlet (AFPAM) 63-113, *Program Protection Planning For Life Cycle Management*, 17 October 2013, 47.

[20] Air Force Instruction (AFI) 23-101, *Materiel Management*, 12 Dec 2016, 250.

[21] Senate Committee On Armed Services. Inquiry Into Counterfeit Electronic Parts, 16.

[22] Global Intellectual Property Center. *Measuring the magnitude of global Counterfeiting Creation of a contemporary global Measure of physical counterfeiting* (U.S. Chamber of Commerce, Washington, D.C. 2016) 4.

[23] Department of Commerce. Defense industrial base assessment:, 7.

[24] IBID., 217.

[25] Senate Committee On Armed Services. Inquiry Into Counterfeit Electronic Parts, 17

[26] Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts. Lanham: Federal Information & News Dispatch, Inc, 2012. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1015153980?accountid=4332. 1.

[27] IBID., 2.

[28] Government Accountability Office, *COUNTERFEIT PARTS DOD Needs to Improve,* GAO Report 16-236, 7.

[29] Government Accountability Office, *DEFENSE SUPPLIER BASE DOD Should*, GAO Report 10-389, 28.

[30] Brian, Grow, "Dangerous Fakes." 1.

[31] Senate Committee On Armed Services. Inquiry Into Counterfeit Electronic Parts, 45.

[32] Schumer: Counterfeiting Of Military Technology Is Putting Troops Lives At Risk And Could Threaten Syracuse Companies Like Lockheed, Src, Sensis, & C Speed - Schumer Pushes Legislation To Crackdown On Makers Of Fake Military Parts. (Lanham: Federal Information & News Dispatch, Inc, 2011. Accessed 25 August 2016), 2.

[33] Department of Justice (DOJ) News Release. *Orange county man sentenced to nearly 16 years For selling subpar flight-critical aircraft parts And for offering to sell fighter plane parts to china.* 29 November 2005, 1.

[34] Senate Committee on The Judiciary. Regarding a hearing on "*counterfeits and their impact on consumer health and safety*" (Washington, D.C. 27 April 2016), 6.

[35] Schumer: Counterfeiting Of Military Technology Is Putting 1.

[36] Jacques S., Gansler, *Addressing Counterfeit Parts in*, 8.

[37] Hans M. Sassenfeld, *Counterfeit Prevention Strategies in the Military,* 6.

[38] Jacques S., Gansler, *Addressing Counterfeit Parts in,* 9.

[39] DOD Instruction (DODI) 4140.67. *DOD Counterfeit Prevention Policy,* 1.

[40] Henry, Livingston, "Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components Recommendations on Policies and Implementation Strategy." BAE Systems, October, 2010. 2.

[41] IBID., 3.

[42] Counterfeit Parts Avoidance & Standards Detection Panel Discussion. SAE International, December 2013, 5.

[43] IBID., 6.

[44] IBID., 13.

[45] Hans M. Sassenfeld, *Counterfeit Prevention Strategies in the Military,* 6.

[46] IBID., 13.

[47] DOD Instruction (DODI) 4140.67. *DOD Counterfeit Prevention Policy,* 1.

[48] Government Accountability Office, *DEFENSE SUPPLIER BASE DOD Should*, GAO Report 10-389, 28.

[49] Henry Livingston, "*Counterfeit Part Reporting Trends Observations in anticipation of forthcoming regulations*" BAE Systems, February, 2014, 3.

[50] DOD Instruction (DODI) 4140.67. *DOD Counterfeit Prevention Policy,* 1.

[51] Government Accountability Office, *COUNTERFEIT PARTS DOD Needs to Improve,* GAO Report 16-236, 9.

[52] IBID., 11.

[53] IBID., 11.

[54] IBID., 14.

[55] IBID., 33.

[56] Ron C. Ball, "The DoD Counterfeit Threat & Compliance." Paper for Keesler Aerospace Solutions, Orlando, FL, 2013, 5.

[57] Air Force Guidance Memorandum (AFGM) to AFI 63-101/20-101. Integrated Life Cycle Management, 16 September 2016, 49.

[58] House. *A Bill to Secure E-Waste Export and Recycling Act*.115th Cong., 2017. HR917 https://www.govtrack.us/congress/bills/115/hr917.

[59] *A Special Report Counterfeit Parts: Increasing Awareness and Developing Countermeasures* (Arlington, VA: Aerospace Industries Association, 2011) 18.

[60] IBID., 15.

[61] Schumer: Counterfeiting Of Military Technology Is Putting 1.

[62] Jacques S., Gansler, *Addressing Counterfeit Parts in,* 44.

[63] Global Intellectual Property Center. *Measuring the magnitude of global Counterfeiting Creation of a contemporary global Measure of physical counterfeiting* (U.S. Chamber of Commerce, Washington, D.C. 2016) 4.

Bibliography

Air Force Instruction (AFI) 23-101. *Materiel Management,* 12 December 2016.

Air Force Guidance Memorandum (AFGM) to AFI 63-101/20-101. Integrated Life Cycle Management, 16 September 2016.

Air Force Pamphlet (AFPAM) 63-113. *Program protection planning for life cycle management*, 17 October 2013.

A Special Report Counterfeit Parts: Increasing Awareness and Developing Countermeasures. Arlington, VA: Aerospace Industries Association, 2011.

Burger, Jim, Henry Livingston, and Tom Sharpe. "Electronic Waste Rules could Help Thwart Flow of Counterfeit Parts." National Defense 99, no. 735 (02, 2015): 14-15. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1653124073?accountid=4332.

Ball, Ron C. "The DoD Counterfeit Threat & Compliance." Paper for Keesler Aerospace Solutions, Orlando, FL, 2013.

Casewell, Greg. "Counterfeit Detection Strategies: When to Do It / How to Do It." Paper for DFR Solutions. College Park, MA, 2015.

Chaudhry, Peggy, and Allan Zimmerman. *Protecting Your Intellectual Property Rights Understanding the Role of Management, Governments, Consumers and Pirates.* Springer, New York: Springer Science & Business Media, 2013.

COUNTERFEIT PARTS DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk. GAO-16-236, Washington, DC: United States Government Accountability Office, February 2016.

Counterfeit Prevention. Lockheed Martin, 2016.

Counterfeit Parts: A Lockheed Martin Perspective. Parts Standardization & Management Committee Conference, Lockheed Martin, 2015.

Counterfeit Parts Avoidance & Standards Detection Panel Discussion. SAE International, December 2013.

Counterfeit Parts Prevention Overview. Honewell, February, 2014.

Defense Contract Management Agency (DCMA) Instruction 1205. *Counterfeit Mitigation*, 6 July 2015.

DEFENSE SUPPLIER BASE DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Needs to Improve Reporting and Oversight to Mitigate Risk of

Counterfeit Parts. GAO-10-389, Washington, DC: United States Government Accountability Office, March 2010.

Department of Commerce. *Defense industrial base assessment: Counterfeit electronics.* Washington D.C.: Bureau of Industry and Security, January 2010.

Dobbs, Andrew. *We Threw Military Electronics In the Trash – China Sold Them Back to Us: How E-Waste Compromises America War tech.* War is Boring, Accessed 24 September 2016. https://medium.com/war-is-boring/we-threw-electronics-in-the-trash-china-sold-them-back-to-us-d52e06111fff.

DOD (DOD) Instruction 4140.67. *DOD Counterfeit Prevention Policy*, 26 April 2013.

DOD (DOD) Instruction 5000.02. *DOD Operation of the Defense Acquisition System*, 7 January 2015.

DOD (DOD) Manual 4140.01. *DOD Supply Chain Materiel Management Procedures: Operational Requirements*, 10 February 2013.

Department of Justice (DOJ) News Release. *Orange county man sentenced to nearly 16 years For selling subpar flight-critical aircraft parts And for offering to sell fighter plane parts to china.* 29 November 2005.

Evans, Gareth Dr. "*Flying fraudulently – how a weak supply chain became the USAF's worst enemy*." Airforce-technology.com, 2012. http://www.airforce technology.com/features/featuresupply-chain-us-air-force-fraudulent-parts/.

Flint, Perry. "All Parts are Not Created Equal." Air Transport World 31, no. 7 (07, 1994): 40. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/224312505?accountid=4332.

Gansler, Jacques S., William Lucyshyn, and John Rigilano. *Addressing Counterfeit Parts in the DoD Supply Chain.* Center for Public Policy and Private Enterprise. College Park, MD: University of Maryland, 2014.

Global Intellectual Property Center. *Measuring the magnitude of global Counterfeiting Creation of a contemporary global Measure of physical counterfeiting*. U.S. Chamber of Commerce, Washington, D.C. 2016.

Grow, Brian, Chi-Chu Tschang, Cliff, Edwards and Brian Burnsed. "Dangerous Fakes." Bloomberg Businessweek, 1 October 2008. http://www.businessweek.com/stories/2008-10-01/dangerous-fakes.

House. *A Bill to Secure E-Waste Export and Recycling Act*.115th Cong., 2017. HR917 https://www.govtrack.us/congress/bills/115/hr917.

Insinna, Valerie. "Proposed Rules on Counterfeit Parts Puts Onus on Industry." National Defense 98, no. 717 (08, 2013): 10. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1429626117?accountid=4332.

Krekel, Bryan, Patton Adams, and George Bakos. "OCCUPYING THE INFORMATION HIGH GROUND: CHINESE CAPABILITIES FOR COMPUTER NETWORK OPERATIONS

AND CYBER ESPIONAGE *." International Journal of Computer Research 21, no. 4 (2014): 333-439. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1682175136?accountid=4332.

Livingston, Henry. "Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components Recommendations on Policies and Implementation Strategy." BAE Systems, October, 2010.

Livingston, Henry. "*Counterfeit Part Reporting Trends Observations in anticipation of forthcoming regulations*" BAE Systems, February, 2014.

Rath, Thomas J. "Tools of Change: Tactical C4ISR and Conflicts-Past, Present, and Future." Air & Space Power Journal 25, no. 2 (Summer, 2011): 100-114. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/918791790?accountid=4332.

Sassenfeld, Hans M. *Counterfeit Prevention Strategies in the Military Supply Chain: Increasing Reliability at a Higher Price*. Capstone, University of Texas, El Paso, 2013.

Senate. Inquiry Into Counterfeit Electronic Parts In The Department Of Defense Supply Chain. 112th Cong., 2nd Sess., 2012. S. Doc. 112-167.

Senate. A resolution recognizing the 70th anniversary and the importance of the Lanham Act by designating July 2016 as "National Anti-Counterfeiting Consumer Education and Awareness Month". 114th Cong., 2nd Sess., 2016. S. Res. 542.

Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts. Lanham: Federal Information & News Dispatch, Inc, 2012. Accessed 25 August 2016. http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1015153980?accountid=4332.

Senate Committee on The Judiciary. Regarding a hearing on "*counterfeits and their impact on consumer health and safety*" Washington, D.C. 27 April 2016.

Schaffer, Mark. "*Development of a Methodology to Determine Risk of Counterfeit Use*." International Electronics Manufacturing Initiative, Herndon, VA. 2013.

Schumer: Counterfeiting Of Military Technology Is Putting Troops Lives At Risk And Could Threaten Syracuse Companies Like Lockheed, Src, Sensis, & C Speed - Schumer Pushes Legislation To Crackdown On Makers Of Fake Military Parts. Lanham: Federal Information & News Dispatch, Inc, 2011. Accessed 25 August 2016.

Shoemaker, Dan and Wilson, Charles. "The Weakest Link - The ICT Supply Chain and Information Warfare." International Conference on Information Warfare and Security. United Kingdom: Academic Conferences International Limited, 2013.